1.0 Summary

Findings and observations: RTF file containing written instructions for some sort of financial scam, clumsily executed. Possible Arabic speaker as author. No dynamic behavior observed myself or via sandbox.

Recommendations: Usual guidelines against opening strange attachments still stand. Admin of the site linking the image might want to review security, specifically around how that file appeared on their site.

Conclusion: Scam message, no apparent malicious activity. Possible that any exploits in this sample might just not be effective running on the current test system.

1.1 Identification

File name: FINANCIAL INTELLIGENCE CENTRE.RTF
File Type: Rich Text Format, Version 1, ANSI
Malware name(s): N/A
Current detection: None (via Virustotal and Malwr)
Malware type: N/A
Size: 9,224,954 bytes
Packer: None
Encryption/encoding: None detected
Origin: Unknown; possible Arabic speaker as author
Compile time: 2014-10-06 08:42

Hashes
MD5: e2e2d91211ed870d44c6df85f58976fe
SHA1: 3d2ec090b308e27e4490a3082901784110e06324
SHA256: 66096c1c1692b8f1a4e8e9b678351601ded0a189241e7cbfeffc01c5bd379b93
ssdeep: 24576:nOowJRsxdhW5DubB5UOG7Pz+UfOowJRsxdhW9DubB5UOG7Pz+UqOowJRsxdhWyDz:I

Test environment details: Win 7 Home Premium SP1 running in VirtualBox 5.0.18_Ubuntu r106667 on Ubuntu 16.04. Hardware is an Acer Aspire 5742 (Intel i3).

1.2 Dependencies

OS: N/A
Imports: N/A
Exports: N/A
Other: RTF reader required

2.0 Characteristics

2.1 Behavior

No dynamic behavior observed besides the link to the seemingly legitimate site for the image in the document.

2.2 Infection

N/A

2.3 Persistence

Nothing observed

2.4 Movement
Nothing observed

2.5 Data Exfiltration
Nothing Observed

2.6 C²
N/A

2.7 Signatures
File name: FINANCIAL INTELLIGENCE CENTRE.rtf
Company: egyptian hak
Operator: PC13
Author: user
Generated with: Microsoft Word 11.0.5604

3.0 Recommendations
Recipients should not open this (or any other) strange document sent to them. Admins of thereach.ca should review this file and its origin.

4.0 Raw Notes

4.1 Static Analysis
Sender: humansettlements001@gmail.com
Subject: IRREVOCABLE PAYMENT ORDER VIA ATM CARD (Please view attached file for details)


```
{\*\generator Microsoft Word 11.0.5604;}{\info{\title FROM: DESK OF: }{\author user}{\operator PC13}{\creatim\yr2014\mo10\dy6\hr8\min42}{\revtim\yr2014\mo10\dy6\hr8\min42}
```

```
{\printim\yr2014\mo6\dy21\hr15\min24}{\version2}{\edmins1}{\nofpages2}{\nofwords715}{\nofchars4082}{\*\company <egyptian hak>}{\nofcharsws4788}{\vern24689}}\margl1810\margr810\margt810\margb0
\widowctrl\ftnbj\aenddoc\noxlattoyen\expshrtn\noultrlspc\dntblnsbdb\nospaceforul\hyphcaps0\horzdoc\dghspace120\dgvspace120\dghorigin1701\dgvorigin1984\dghshow0\dgvshow3\jcompress\viewkind1\views
\sectd \linex0\sectdefaultcl\sectrsid8596735\sftnbj {\*\pnseclvl1\pnucrm\pnstart1\pnindent720\pnhang {\pntxta .}}{\*\pnseclvl2\pnucltr\pnstart1\pnindent720\pnhang {\pntxta .}}{\*\pnseclvl3\pndec
\pnlcltr\pnstart1\pnindent720\pnhang {\pntxta )}}{\*\pnseclvl5\pndec\pnstart1\pnindent720\pnhang {\pntxtb (}{\pntxta )}}{\*\pnseclvl6\pnlcltr\pnstart1\pnindent720\pnhang {\pntxtb (}{\pntxta )}}{
```

```
{\sp{\sn pibName}{\sv http://www.thereach.ca/images/South%20African%20High%20Commission%20logo.jpg}}{\sp{\sn pibFlags}{\sv 10}}{\sp{\sn fRecolorFillAsPicture}{\sv 0}}{\sp{\sn
http://www.thereach.ca/images/South%20African%20High%20Commission%20logo.jpg}}{\sp{\sn fLayoutInCell}{\sv 1}}{\sp{\sn fBehindDocument}{\sv 1}}{\sp{\sn fPseudoInline}{\sv 0}}{\
\ql \li0\ri0\widctlpar\pvpara\posnegx-160\posnegy-252\dxfrtext180\dfrmtxtx180\dfrmtxty0\aspalpha\aspnum\faauto\adjustright\rin0\lin0\itap0 {\pict\picscalex20\picscaley13\piccr
\picw14737\pich19368\picwgoal8355\pichgoal10980\wmetafile8\bliptag1001683203\blipupi96{\*\blipuid 3bb479037c41d386fb031f3f39599ede}
```


4.2 Dynamic Analysis

Human Settlements
FINANCIAL INTELLIGENCE CENTRE (FIC)
REPUBLIC OF SOUTH AFRICA

Office No: 7 Kikuyu Road Sunninghill
Sandton Gauteng
South Africa.
Tel/fax: +2786 663 7851.

Dear Email Owner/Fund Beneficiary,

IRREVOCABLE PAYMENT ORDER VIA ATM CARD

within the Next Three (3) Banking Working days from today. So if you like to receive your funds through this means you're advised to contact **(Dr. Adams Omar Nkosi)** and forward him the following information as stated below:

1. Your Full Name:
2. Address Where You Want the Courier Company to Send Your ATM Card To or (P.O Box)
3. Your Age:
4. Occupation:
5. Email Address:
6. Cell/Mobile Number:

NOTE: You are advised to furnish **Dr. Adams Omar Nkosi** with your correct and valid details. Also be informed that the amount to be paid to you now is **ONE MILLION BRITISH POUNDS (GBP£1,000,000.00) ONLY**. We expect your urgent response to this email as to enable us monitor this payment effectively thereby making contact with **Dr. Adams Omar Nkosi** as directed to avoid further delay.

Please Be Warned, as The United Nations Anti-Crime Commission and the International Monetary Fund (IMF) does not instruct any other Bank or agent in this payment except **(Dr. Adams Omar Nkosi)**, whom we can only give attention to, and from now, we advice you to stop all the communications you are having with any other Agent or bank officials in Europe, Asia and Africa regarding to your payment.

Thanks for your understanding as you follow instructions.

A. Lincoln

Yours in Services.

MR. ANDREW MOOR
PUBLIC INFORMATION OFFICER.
(FIC) SOUTH AFRICA.

4.3 Disassembly
No successful disassembly

4.4 Debugging
N/A

4.5 Other
N/A